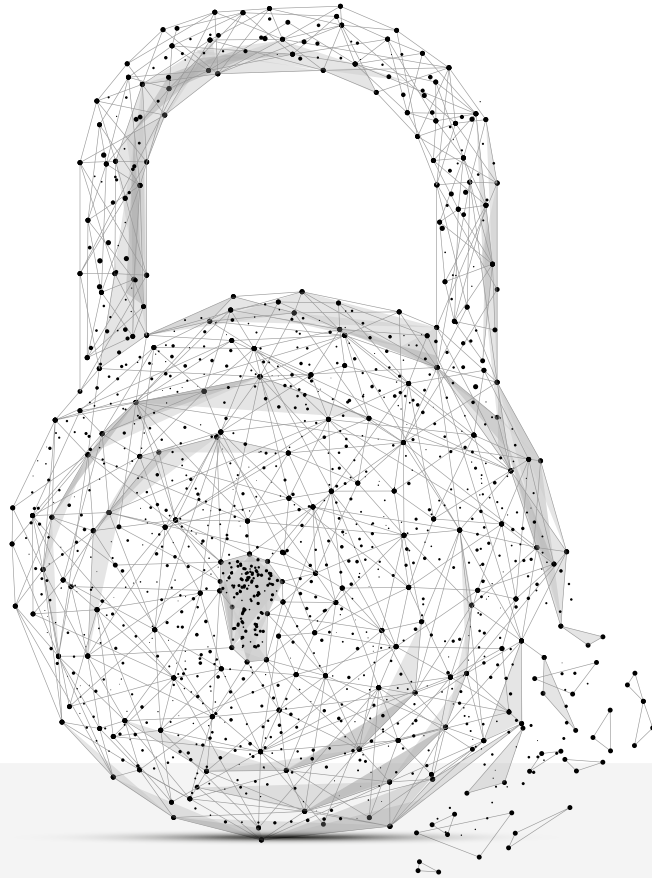
Piotr Drobek - zastępca dyrektora Departamentu Edukacji Społecznej i Współpracy Międzynarodowej, przewodniczący Zespołu do spraw reformy prawa ochrony danych osobowych w Unii Europejskiej w Biurze GIODO.

Na stronie Ministerstwa Cyfryzacji 28 marca br. pojawił się projekt ustawy o ochronie danych osobowych. Jak dużo pracy czeka Ministerstwo, odnośnie do zmian w przepisach?

Piotr Drobek: Reforma ochrony danych osobowych jest procesem kompleksowym i wymaga rzetelnego przeglądu obowiązujących w Polsce przepisów prawa, tak by wszystkie akty prawne regulujące przetwarzanie danych osobowych w Polsce były 25.5.2018 r. zgodne z ogólnym rozporządzeniem o ochronie danych osobowych. I to jest owo niesłychanie duże zadanie – rewizja sektorowych przepisów w zakresie ochrony danych osobowych. Jednocześnie polski ustawodawca musi zapewnić, że rozpoczęcie stosowania ogólnego rozporządzenia o ochronie danych nie spowoduje istnienia luk regulacyjnych w stosunku do obecnego stanu prawnego, a obecne lub planowane przepisy sektorowe będą zgodne z ogólnym rozporządzeniem. Niewątpliwie wymaga to od Ministerstwa Cyfryzacji koordynacji działań legislacyjnych w bardzo szerokim zakresie. Podkreślenia wymaga jednak fakt, że te branżowe postanowienia nie mogą obniżać poziomu ochrony danych określonego przepisami rozporządzenia. Należy więc bardzo roztropnie podchodzić do wszelkiego rodzaju ograniczeń jego stosowania przez poszczególne branże, tak by wartość uzasadniająca takie ograniczenie naszych praw i wolności była precyzyjnie wskazana – to swojego rodzaju test niezbędności takiego ograniczenia. Niezbędności w demokratycznym państwie prawa.

Jeżeli zaś chodzi o samo ogólne rozporządzenie o ochronie danych, to większość jego przepisów będzie stosować się bezpośrednio we wszystkich państwach członkowskich. Co więcej, nie może być w żaden sposób implementowana do prawa krajowego ani nawet interpretowana przez ustawodawcę krajowego.

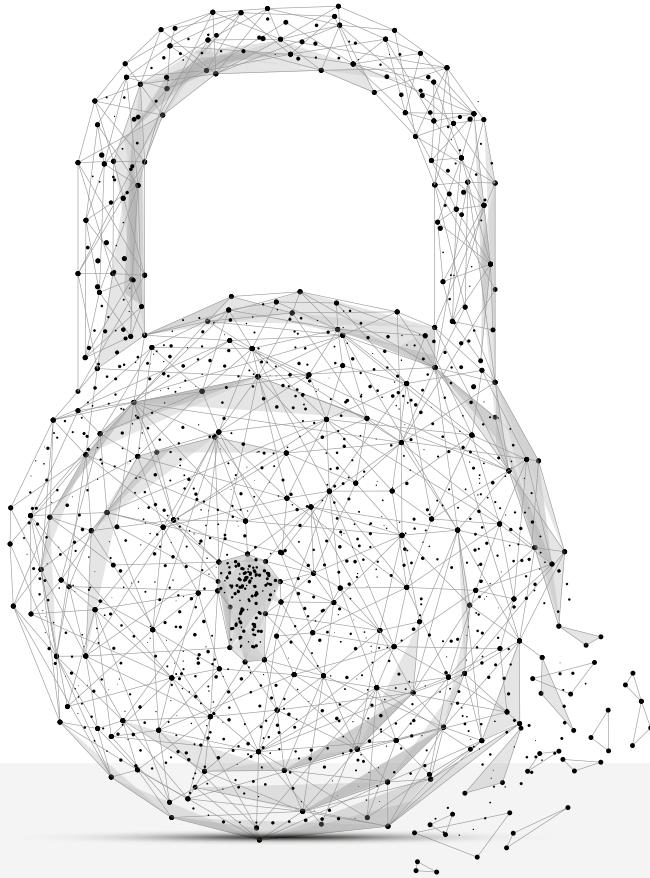


Oznacza to, że polski ustawodawca ma tutaj bardzo ograniczony zakres działań legislacyjnych. Innymi słowy, w polskim porządku prawnym można przyjąć tylko takie przepisy prawa, bez których nie byłoby możliwe właściwe wdrożenie rozporządzenia. Niemniej w akcie tym znajdziemy ok. 60 przepisów, określających obszary, które można odrębnie uregulować w prawie krajowym. Mamy w tej grupie przepisy dotyczące m.in. pozycji ustrojowej polskiego organu ochrony danych, administracyjnych kar pieniężnych dla sektora publicznego czy możliwe obniżenie wieku dziecka, które może wyrazić zgodę na przetwarzanie jego danych osobowych w usługach społeczeństwa informacyjnego. To kolejne wyzwanie dla polskiego ustawodawcy. Ważne, by proces stanowienia prawa w tym obszarze był całkowicie transparentny i uwzględniał stanowiska wszystkich interesariuszy, w tym GIODO. Obchodzimy w tym roku 20-lecie ochrony danych osobowych w Polsce. Nie sposób nie dostrzegać tak pokaźnego doświadczenia GIODO w budowaniu polskiego systemu ochrony danych w kontekście obecnej unijnej reformy.

Warto też dodać, że pakiet reformujący ramy prawne ochrony danych osobowych w UE obejmuje nie tylko ogólne roz-porządzenie o ochronie danych (rozporządzenie 2016/679), lecz także dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/680 z 27.4.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez wła-ściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW. Z tego względu właściwe wdrożenie nowych ram prawnych powinno uwzględniać oba akty prawne tak, aby przyszły system ochrony danych osobowych był spójny, co wymaga właściwej koordynacji tych działań w obrębie rządu.

Kiedy, według Pana, nowa ustawa o ochronie danych osobowych weszłaby w życie?

P.D.: Na pewno datą nieprzekraczalną jest 25.5.2018 r., czyli dzień, w którym rozpocznie się stosowanie rozporządzenia o ochronie danych osobowych. Nie wolno jednak zapominać, że na ten moment trzeba właściwie przygotować Biuro GIODO. Pracujemy już nad optymalną strukturą, tak by GIODO był gotowy do wykonywania nowych obowiązków. Niezbędne jest w tym kontekście również przygotowanie projektu budżetu na rok 2018, co powoduje, że kształt przepisów nowej ustawy o ochronie danych osobowych, niezależnie od terminu jej wejścia w życie, powinniśmy znać odpowiednio wcześnie.



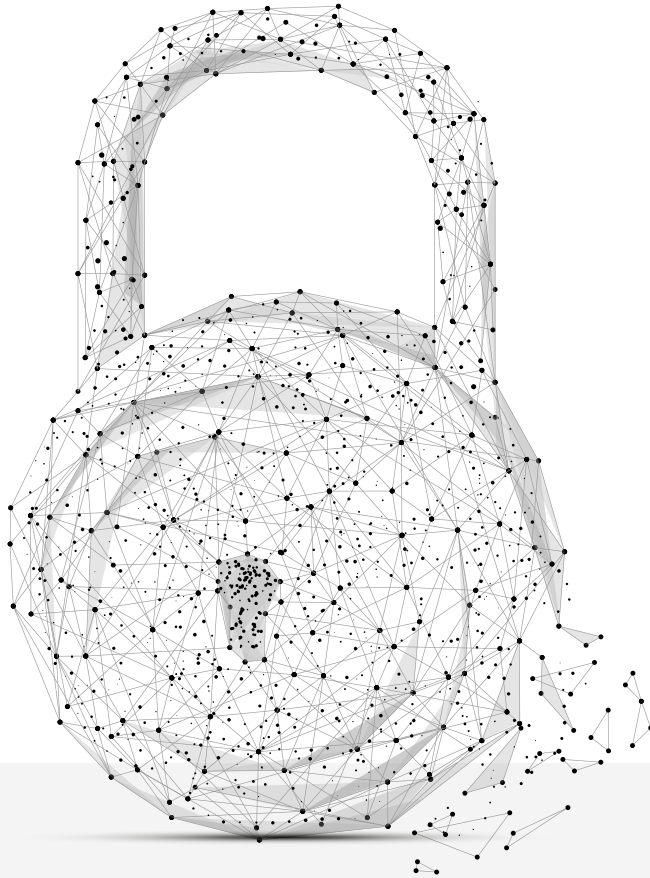
Projekt przewiduje powołanie nowego urzędu, nowego prezesa, czy coś poza zmianą nazwy będzie się kryło?

P.D.: Przedstawiony przez Ministerstwo Cyfryzacji projekt, zwłaszcza że jest szczątkowy, traktujemy jako otwarcie dyskusji. Już najwyższy czas, żeby się rozpoczęła, zwłaszcza w tak kluczowych dla całego systemu ochrony danych osobowych kwestiach, jak np. niezależność organu ochrony danych osobowych. Nie wyobrażam sobie, że powołujemy zupełnie nowy organ, a obecny będziemy likwidować. GIODO od dwudziestu lat stoi na straży podstawowych praw człowieka, jakimi są prawo do ochrony danych osobowych i prawo do prywatności. Owe 20 lat działalności to ogromna wiedza, długoletnia praktyka, długotrwała współpraca z innymi organami ochrony danych osobowych w Europie i na świecie, zaangażowanie w prace nad reformą ochrony danych oraz wdrożeniem rozporządzenia na polu krajowym i europejskim. Dotychczasowe doświadczenia zagraniczne pokazują, że nowych rozwiązań nie można tworzyć w oderwaniu od wiedzy i doświadczenia funkcjonującego już organu ochrony danych.

W przedstawionym przez Ministerstwo Cyfryzacji projekcie ustawy pada jedynie nowa nazwa polskiego organu, co rodzi różne zbędne spekulacje dotyczące kształtu i przyszłości GIODO. Choć kwestia nazwy nie jest kluczowa dla procesu wdrożenia przepisów ogólnego rozporządzenia, to jednak przedstawione przez Ministerstwo Cyfryzacji uzasadnienie dla takiej zmiany nie wydaje się przekonujące. W czasie prac nad polskim tekstem ogólnego rozporządzenia ustawodawca europejski świadomie nawiązał do rozwiązań funkcjonujących od kilkunastu już lat w prawie UE. Otóż zgodnie z rozpo-rządzeniem nr 45/2001 organem nadzorczym w zakresie przetwarzania danych osobowych przez organy i instytucje unijne jest Europejski Inspektor Ochrony Danych, a w poszczególnych organach lub instytucjach powołuje się inspektorów ochrony danych (ang. data protection officers). Również w polskim prawie można podać przykład Głównego Inspektora Pracy, inspektorów pracy czy wreszcie społecznych inspektorów pracy. Podobne w gruncie rzeczy nazwy jak dotąd nie powodowały żadnych konfuzji.

Warto też zadać sobie pytanie o koszty takiej zmiany – finansowe, prawne, a także społeczne, dotyczące rozpoznawalności GIODO w świadomości obywateli, przedsiębiorców i administracji publicznej. Decyzja o zmianie nazwy organu powinna być więc elementem szerszej dyskusji i uwzględniać powyższe wątpliwości. Czy stać nas na taki koszt, w sytuacji kiedy taka zmiana nie wydaje się konieczna?

Obecny model funkcjonowania GIODO pod względem statusu i gwarancji niezależności zapewnia bardzo wysokie stan-dardy i spełnia wymogi stawiane organom nadzorczym przepisami rozporządzenia. Konieczność ich wdrożenia nie powinna tych standardów obniżać. Taki pogląd znalazł również potwierdzenie w bardzo wyraźnej linii orzeczniczej Trybunału Sprawiedliwości oraz został wyrażony w doktrynie – vide artykuł autorstwa Krzysztofa Rokity w „Europejskim Przeglądzie Sądowym" 2016, Nr 7.



Z całą pewnością organ ochrony danych osobowych nie może być sprowadzony do roli organu regulacyjnego mediują-cego między różnymi interesariuszami. Musi być organem, którego głównym celem jest ochrona praw podstawowych jednostek.

W uzasadnieniu projektu opisane zostały kwestie kontroli. Czym różnią się one od kontroli, które obecnie przebiegają?

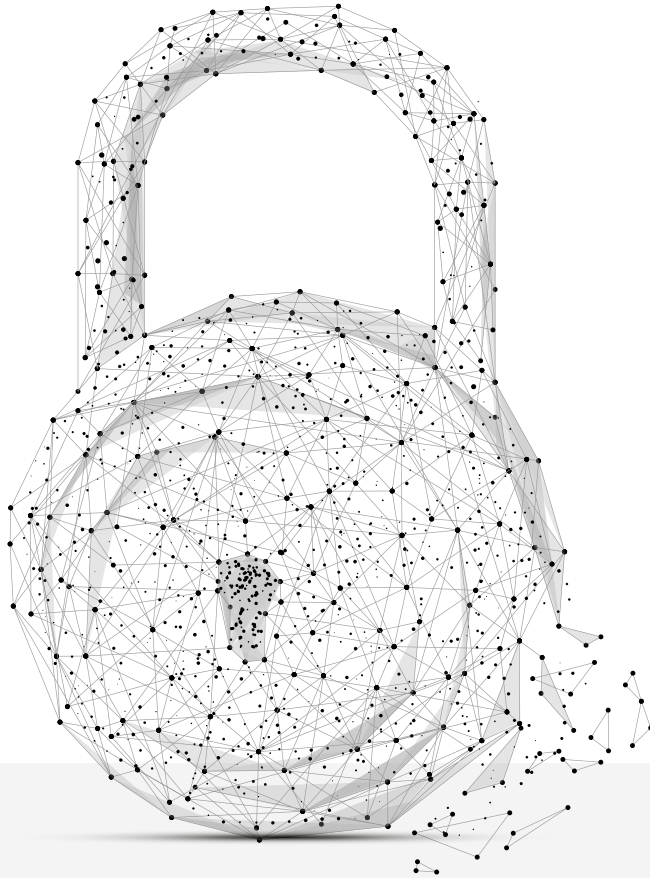
P.D.: Już niebawem GIODO zaprezentuje projekt przepisów regulujących prowadzenie czynności kontrolnych przez pra-cowników GIODO. Wykorzystując nasze wieloletnie doświadczenie w tym zakresie, chcemy zaprezentować modelowe podejście do tego zagadnienia, uwzględniające przede wszystkim rozwiązania przewidziane przepisami unijnego rozporzą-dzenia, takie jak możliwość przeprowadzenia wspólnych kontroli z innymi organami nadzorczymi UE.

Projekt przewiduje wprowadzenie kar. Jak GIODO widzi te 20 milionów euro w skali polskiego przedsiębiorstwa oraz w administracji publicznej?

P.D.: Unijne rozporządzenie przewiduje możliwość nakładania przez organy nadzorcze państw członkowskich UE na podmioty naruszające zasady ochrony danych osobowych wysokich kar finansowych. Dzięki temu każdy organ nadzorczy państwa członkowskiego stojący na straży danych osobowych będzie równie silny i będzie mógł nałożyć karę wynoszącą maksymalnie do 4% całkowitego rocznego światowego obrotu lub 20 milionów euro. To bardzo dotkliwa sankcja, która ma z założenia działać dyscyplinująco i odstraszająco. Pamiętajmy jednak, że rozporządzenie określa maksymalne wysokości kar, przy ich wymierzaniu zaś pod uwagę ma być branych wiele czynników. Myślę, że wobec takiej groźby nawet giganci zaczną traktować dane europejskich obywateli z należytą troską.

Wbrew wcześniej składanym deklaracjom resort cyfryzacji proponuje całkowite wyłączenie stosowania administracyj-nych kar pieniężnych wobec organów publicznych (w rozumieniu art. 5 § 2 pkt 3 ustawy – Kodeks postępowania admini-stracyjnego) oraz większości podmiotów publicznych (w rozumieniu art. 9 pkt 17 ustawy o finansach publicznych). Rów-nocześnie zaś w stosunku do pozostałych podmiotów publicznych ujętych w ustawie o finansach publicznych sugeruje zmniejszenie maksymalnego wymiaru administracyjnej kary pieniężnej do wysokości CZTERYSTUKROTNIE niższej od przewidzianej w rozporządzeniu.

Rozważając kwestię wysokości kar, powinniśmy przede wszystkim mówić o równości podmiotów. Jaka jest różnica mię-dzy szpitalem publicznym a prywatnym, w sytuacji gdy doszło w nich do wycieku danych osobowych pacjentów? Z per-spektywy osób, których dane zostały utracone,



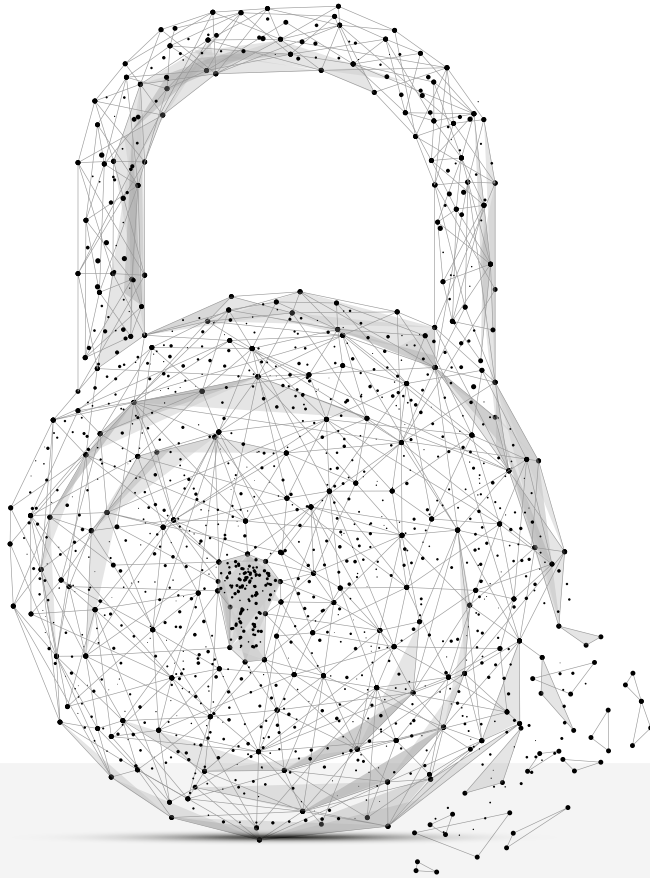
sytuacja jest taka sama. I jeden, i drugi podmiot utracił władztwo nad danymi, a pacjenci ponieśli taką samą szkodę. Dodatkowo warto zaznaczyć, że do tej pory w sektorze publicznym poziom zgodności z przepisami o ochronie danych osobowych zazwyczaj był wyższy niż w sektorze prywatnym. Czy tak będzie dalej – nie wiadomo.

Zmiany dotyczą również ABI, co się najbardziej zmieni w jego pracy?

P.D.: Warto podkreślić, że wprowadzona w 2015 r. nowelizacja ustawy o ochronie danych osobowych, zmieniając przepisy dotyczące administratorów bezpieczeństwa informacji, uwzględniała rozwiązania przewidywane w unijnym rozporządzeniu. Umożliwiło to osobom sprawującym funkcję ABI przygotowanie się do wymogów określonych ogólnym rozporządzeniem o ochronie danych. Wykonując wiele swoich nowych obowiązków, zdobywali oni doświadczenie i poszerzali swoją wiedzę. Upowszechniali również wiedzę o zasadach i obowiązkach w zakresie ochrony danych osobowych w swoich organizacjach, często zyskując coraz większe zrozumienie i wsparcie u kadry zarządzającej oraz wśród pracowników.

Większość obowiązków i zadań przyszłego inspektora będzie tożsama z obecnie wykonywanymi przez ABI. Biorąc jed-nak pod uwagę fakt, że rozporządzenie wprowadza istotne zmiany w systemie ochrony danych osobowych, czyniąc administratora danych podmiotem w większym niż dotąd stopniu odpowiedzialnym za zgodne z prawem przetwarzanie danych osobowych, to automatycznie rola i zadania wspierającego go w tym inspektora ochrony danych ulegną pewnej modyfikacji.

Jedno jest jednak pewne – znaczenie inspektorów dla całego systemu zapewniania zgodności z przepisami o ochronie danych jeszcze wzrośnie i taki wniosek płynie z przygotowanych przez GIODO oraz Grupę Roboczą Art. 29 Wytycznych dotyczących inspektorów ochrony danych, których polska wersja jest już dostępna na stronie GIODO. W dokumencie rozwiewamy wątpliwości dotyczące sytuacji obligatoryjnego wyznaczenia inspektora ochrony danych, opisujemy jego rolę w organizacji i zadania, jakie są stawiane osobom sprawującym tę funkcję. Są to bardzo pomocne wskazówki dla wszystkich, którzy od maja 2018 r. będą musieli bądź będą chcieli powołać inspektora ochrony danych. Serdecznie zapraszamy do lektury tego dokumentu.



Z punktu widzenia sektora publicznego, na co jeszcze warto zwrócić uwagę w ogólnym rozporządzeniu o ochronie danych osobowych?

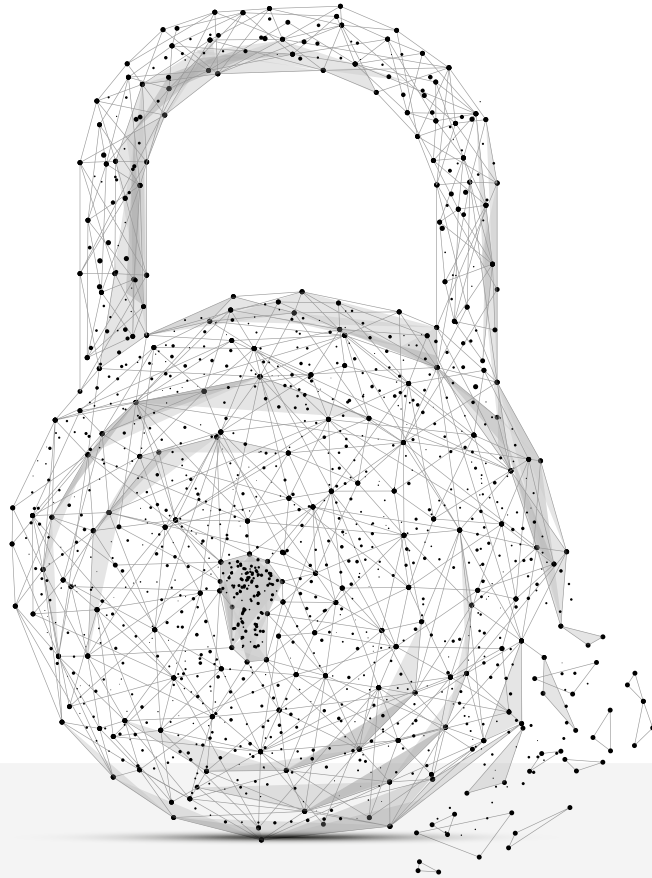
P.D.: Unijne rozporządzenie o ochronie danych osobowych co do zasady w takim samym stopniu odnosi się i do przedsię-biorców, i do administracji publicznej. Zatem zarówno przedsiębiorcy, jak i podmioty z sektora administracji publicznej – będący administratorami danych osobowych zobowiązanymi do ich ochrony – powinni mieć świadomość, że od 25.5.2018 r., a więc od dnia, w którym we wszystkich państwach członkowskich UE rozporządzenie zacznie być bezpośrednio stosowane, w systemie ochrony danych osobowych nastąpią poważne zmiany. W tym kontekście warto jednak wskazać na jedną kwestię, otóż administratorzy danych i podmioty przetwarzające będące organami lub podmiotami publicznymi (z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości) będą mieli obowiązek wyznaczenia inspektora ochrony danych.

Na czym polegać będzie korzyść certyfikacji?

P.D.: Kwestia certyfikacji to osobne, obszerne zagadnienie, wymagające omówienia w wielu aspektach, a także w odniesieniu do tego, co dzieje się w tym zakresie na rynku europejskim. Ponadto na temat certyfikacji trwa również dyskusja na spotkaniach w Grupie Roboczej Art. 29 GIODO kończy obecnie przygotowanie osobnej analizy w tym zakresie, więc chętnie wrócimy do tego tematu w osobnej rozmowie. Mechanizm certyfikacji z całą pewnością może być doskonałym narzędziem do wykazania zgodności z przepisami rozporządzenia, szczególnie wobec braku wyraźnych wskazówek dotyczących sposobów zabezpieczania danych i dokumentacji z tym związanej oraz faktu, że przestaną obowiązywać zasady określone w rozporządzeniu technicznym do polskiej ustawy o ochronie danych.

Na co chciałby Pan zwrócić szczególną uwagę w odniesieniu do konstruowania nowego krajowego systemu ochrony danych osobowych?

P.D.: GIODO kilka miesięcy temu zainicjował dyskusję nad przyszłym kształtem procedur przed organem ochrony danych osobowych. Wstępne zaprezentowane wtedy propozycje mogą być traktowane jako kontrowersyjne, lecz były one nowatorską i spójną próbą zapewnienia efektywności organu ochrony danych, który stojąc na straży praw osób, zawsze będzie się borykał z ograniczonymi zasobami. Jednocześnie nie można pominąć faktu, że działania nadzorcze organu ochrony danych wpisują się w szerszy system narzędzi i instytucji mających na celu zapewnienie zgodności z przepisami rozporządzenia. Wśród nich warto wskazać na novum w postaci sądowego trybu dochodzenia praw z zakresu ochrony danych czy mechanizmy certyfikacyjne, a także na zmodyfikowany instrument, jakim są kodeksy postępowania (dotychczasowe kodeksy dobrych praktyk).



Jak inne kraje unijne przeprowadzają reformę ochrony danych osobowych?

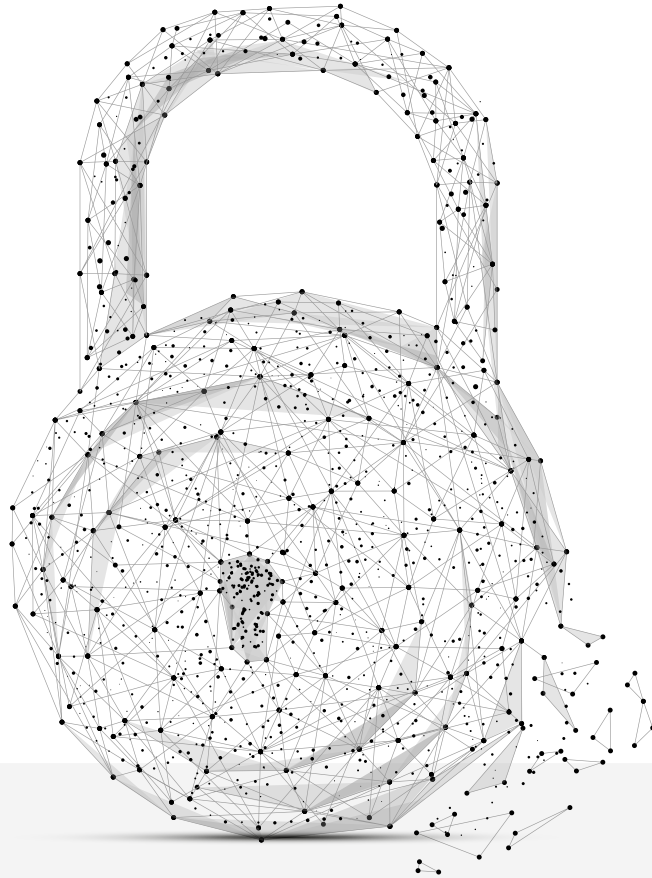
P.D.: Każdy z krajów członkowskich pracuje nad projektem przepisów krajowych niezbędnych dla kompleksowego wdro-żenia unijnej reformy ochrony danych. Nie mniej ważne w tym kontekście jest zaangażowanie unijnych organów nadzor-czych w przygotowywanie administratorów danych do stosowania rozporządzenia. Żeby administratorom danych w Polsce ułatwić wypełnienie nowych obowiązków wynikających z rozporządzenia, a jednocześnie umożliwić im lepsze przygotowanie się do stosowania nowych regulacji, polski organ ochrony danych wspólnie z innymi europejskimi rzecznikami skupionymi w Grupie Roboczej Art. 29 zaprezentował już i poddał konsultacjom Wytyczne dotyczące takich zagadnień, jak: prawo do przenoszenia danych, wyznaczanie inspektora ochrony danych oraz ustalanie wiodącego organu nadzorczego. Wytyczne dotyczące oceny skutków dla ochrony danych to kolejny tego typu dokument, który został opracowany i zaprezentowany przez GIODO. Wszystkie te dokumenty zawierają konkretne wskazówki i przykłady zastosowania instrumentów prawnych przewidzianych przepisami unijnego rozporządzenia o ochronie danych osobowych, które będą stosowane od 25.5.2018 r.

Jak na takiej zmianie systemu ochrony danych osobowych w całej Europie skorzysta szary obywatel?

P.D.: Rozporządzenie przeciętnemu obywatelowi zapewni wzmocnienie jego praw. Przykładowo będzie on mógł przenosić swoje dane między administratorami, skorzystać z prawa do bycia zapomnianym, a także prawa do uzyskania odszkodowania. Ponadto o swoich prawach powinien on być lepiej informowany.

Warto też wspomnieć o rozwiązaniach, które wzmocnią ochronę naszej prywatności, a wiążą się z obowiązkami nałożo-nymi na administratorów danych. Myślę tu o dwóch mechanizmach – privacy by design (prywatność w fazie projektowa-nia), zakładający, że narzędzia i usługi powinny być tak konstruowane, by od samego początku uwzględniały potrzebę ochrony prywatności obywateli, oraz privacy by default (prywatność w ustawieniach domyślnych). Mechanizm ten wska-zuje, iż podstawowe ustawienia powinny chronić prywatność użytkownika, gromadzić minimalny zakres danych osobo-wych i dawać mu swobodę decydowania w tym zakresie.

Rozwinięciem praktycznych aspektów ochrony prywatności w fazie projektowania jest zaś dokonywanie oceny ryzyka i skutków wpływu projektu na prywatność oraz poziom ochrony danych (privacy impact assessment). Do jej przeprowadza-nia administrator danych lub podmiot przetwarzający są zobowiązani wówczas, gdy operacje przetwarzania stwarzają szczególne ryzyko dla praw i wolności podmiotów danych z racji



swego charakteru, zakresu lub celów. Żeby przynosiła ona oczekiwane rezultaty, powinna być przeprowadzana, jeszcze zanim jakieś urządzenia czy systemy zostaną wprowadzone do użycia. Ważne jest, by zakres dokonywanej oceny był szeroki i wykraczający poza problemy ściśle prawne oraz by odbywała się ona w sposób systematyczny.

Czy coś jeszcze ulegnie rewolucyjnej zmianie?

P.D.: O nowych przepisach często mówi się jako o rewolucji, lecz pamiętajmy, że jednak w dużym stopniu bazują one na dotychczasowym dorobku w tej dziedzinie w Europie, w tym w Polsce. Czyli nie powstały one w próżni, lecz są efektem rozwoju i praktycznego stosowania dotychczasowych koncepcji i instytucji prawnych.

Najważniejszy z punktu widzenia działania systemu ochrony danych osobowych jest fakt, iż podstawowe zasady prze-twarzania danych i podstawy prawne dla operacji przetwarzania, a więc najważniejsze wartości tego systemu, zostały utrzymane. Zmienia się jedynie podejście do sposobu dbania o bezpieczeństwo danych osobowych i instrumenty prawne mające służyć takiemu bezpieczeństwu.

I tak, dla administratorów danych ogólne rozporządzenie o ochronie danych niesie przede wszystkim zmianę podejścia do systemu zarządzania ochroną przetwarzanych informacji. To na nich bowiem przenosi się ciężar odpowiedzialności za przestrzeganie zasad i obowiązków wynikających z nowych przepisów. Próżno w rozporządzeniu szukać konkretnych wskazówek dotyczących wymaganych zabezpieczeń technicznych. Zamiast szczegółowej regulacji wszystkich procesów przetwarzania danych mamy podejście oparte na ryzyku. Wszystko w zamyśle nakłada na administratora najważniejszy obowiązek wykazania, że zastosował odpowiednie środki organizacyjne i techniczne oraz że to, jak przetwarza dane osobowe, spełnia wymagania ogólnego rozporządzenia o ochronie danych i oczekiwania GIODO.
obronnym.